Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. – 30. (Canceled).

31. (New) A method, comprising:

selecting a severity level for a controller the severity level being selected from a plurality of available severity levels that at least include:

a) a first severity level that indicates the existence of an anomaly that an application can recover from, said application also able to perform a desired task notwithstanding the anomaly;

b) a second severity level that indicates the existence of an error that an application can recover from, said application also being unable to perform a desired task because of the error;

said selecting of said severity level including selecting one of a), b) above

instantiating a logging controller from the controller, the logging controller inheriting the severity level from the controller, the logging controller to receive logging messages from various categories of software within an enterprise information system, the logging messages having varied levels of severity, the logging controller designed to write into a log file those of the received logging messages having a severity level that is higher than a first maximum severity level setting, the logging controller designed to not write into the log file those of the received logging messages having a severity level that is lower than a first minimum severity

level setting, the inherited severity level being below said first maximum severity level setting and above said first minimum severity level setting;

instantiating a tracing controller from the controller, the tracing controller inheriting the severity level from the controller, the tracing controller to receive tracing messages from various software locations within the enterprise information system, the tracing messages having varied levels of severity, the tracing controller designed to write into a trace file those of the received tracing messages having a severity level that is higher than a second maximum severity level setting, the tracing controller designed to not write into the trace file those of the received tracing messages having a severity level that is lower than a second minimum severity level setting, the inherited severity level being below said second maximum severity level setting and above said second minimum severity level setting;

setting the first and second maximum and minimum security levels of the respective logging and tracing controllers equal to the inherited severity level to configure the logging and tracing controllers to write into their respective log and trace files messages whose severity level is above the inherited severity level and not write into their respective log and trace files messages whose severity level is below the inherited severity level;

subsequent to said logging and tracing controllers writing received messages into their respective log and trace files, correlating the specific locations of software within the enterprise information system to the specific categories of software within the enterprise information system; and,

informing the logging controller that the logging controller is to write received messages into both the log file and the trace file so that the tracing controller is no longer used to write received tracing messages into the trace file.

32. (New) The method of claim 31 wherein the available security levels further include:

a third severity level whose corresponding messages contain information for debugging;

a fourth severity level that permits its corresponding messages to contain path information for looping and branching;

a fifth severity level whose messages are an echo of what has been performed.

33. (New) The method of claim 32 wherein the first and second severity levels are higher severity than the third, fourth and fifth severity levels.

34. (New) The method of claim 33 wherein respective severity levels for at least a portion of the received logging and tracing messages are determined by assigning the respective severity levels to the respective software within the enterprise system that generated the portion of the received logging and tracing messages.

35. (New) The method of claim 34 wherein the correlating of the specific locations of software within the enterprise information system to specific categories of software within the enterprise information system is submitted through a category application programming interface (API).

36. (New) The method of claim 35 wherein the informing of the logging controller that the logging controller is to write received messages into both the log file and the trace file is

conducted through the messages received by the logging controller that are written into both the log file and the trace file.

37. (New) An article of manufacture comprising program code stored on a computer readable storage medium, said program code to be read from said computer readable storage medium and processed by one or more processors to perform a method, comprising:

selecting a severity level for a controller the severity level being selected from a plurality of available severity levels that at least include:

a) a first severity level that indicates the existence of an anomaly that an application can recover from, said application also able to perform a desired task notwithstanding the anomaly;

b) a second severity level that indicates the existence of an error that an application can recover from, said application also being unable to perform a desired task because of the error;

said selecting of said severity level including selecting one of a), b) above

instantiating a logging controller from the controller, the logging controller inheriting the severity level from the controller, the logging controller to receive logging messages from various categories of software within an enterprise information system, the logging messages having varied levels of severity, the logging controller designed to write into a log file those of the received logging messages having a severity level that is higher than a first maximum severity level setting, the logging controller designed to not write into the log file those of the received logging messages having a severity level that is lower than a first minimum severity

level setting, the inherited severity level being below said first maximum severity level setting and above said first minimum severity level setting;

instantiating a tracing controller from the controller, the tracing controller inheriting the severity level from the controller, the tracing controller to receive tracing messages from various software locations within the enterprise information system, the tracing messages having varied levels of severity, the tracing controller designed to write into a trace file those of the received tracing messages having a severity level that is higher than a second maximum severity level setting, the tracing controller designed to not write into the trace file those of the received tracing messages having a severity level that is lower than a second minimum severity level setting, the inherited severity level being below said second maximum severity level setting and above said second minimum severity level setting;

setting the first and second maximum and minimum security levels of the respective logging and tracing controllers equal to the inherited severity level to configure the logging and tracing controllers to write into their respective log and trace files messages whose severity level is above the inherited severity level and not write into their respective log and trace files messages whose severity level is below the inherited severity level;

subsequent to said logging and tracing controllers writing received messages into their respective log and trace files, correlating the specific locations of software within the enterprise information system to the specific categories of software within the enterprise information system; and,

informing the logging controller that the logging controller is to write received messages into both the log file and the trace file so that the tracing controller is no longer used to write received tracing messages into the trace file.

38. (New) The article of manufacture of claim 37 wherein the available security levels further include:

a third severity level whose corresponding messages contain information for debugging;

a fourth severity level that permits its corresponding messages to contain path information for looping and branching;

a fifth severity level whose messages are an echo of what has been performed.

39. (New) The article of manufacture of claim 38 wherein the first and second severity levels are higher severity than the third, fourth and fifth severity levels.

40. (New) The article of manufacture of claim 39 wherein respective severity levels for at least a portion of the received logging and tracing messages are determined by assigning the respective severity levels to the respective software within the enterprise system that generated the portion of the received logging and tracing messages.

41. (New) The article of manufacture of claim 40 wherein the correlating of the specific locations of software within the enterprise information system to specific categories of software within the enterprise information system is submitted through a category application programming interface (API).

42. (New) The article of manufacture of claim 41 wherein the informing of the logging controller that the logging controller is to write received messages into both the log file and the trace file is conducted through the messages received by the logging controller that are written into both the log file and the trace file.

43. (New) A computer comprising program code stored in memory of said computer system, said memory coupled to one or more processors of said computing system, said program code to be read from said memory and processed by said one or more processors to perform a method, comprising:

selecting a severity level for a controller the severity level being selected from a plurality of available severity levels that at least include:

a) a first severity level that indicates the existence of an anomaly that an application can recover from, said application also able to perform a desired task notwithstanding the anomaly;

b) a second severity level that indicates the existence of an error that an application can recover from, said application also being unable to perform a desired task because of the error;

said selecting of said severity level including selecting one of a), b) above

instantiating a logging controller from the controller, the logging controller inheriting the severity level from the controller, the logging controller to receive logging messages from various categories of software within an enterprise information system, the logging messages having varied levels of severity, the logging controller designed to write into a log file those of the received logging messages having a severity level that is higher than a first maximum

severity level setting, the logging controller designed to not write into the log file those of the received logging messages having a severity level that is lower than a first minimum severity level setting, the inherited severity level being below said first maximum severity level setting and above said first minimum severity level setting;

instantiating a tracing controller from the controller, the tracing controller inheriting the severity level from the controller, the tracing controller to receive tracing messages from various software locations within the enterprise information system, the tracing messages having varied levels of severity, the tracing controller designed to write into a trace file those of the received tracing messages having a severity level that is higher than a second maximum severity level setting, the tracing controller designed to not write into the trace file those of the received tracing messages having a severity level that is lower than a second minimum severity level setting, the inherited severity level being below said second maximum severity level setting and above said second minimum severity level setting;

setting the first and second maximum and minimum security levels of the respective logging and tracing controllers equal to the inherited severity level to configure the logging and tracing controllers to write into their respective log and trace files messages whose severity level is above the inherited severity level and not write into their respective log and trace files messages whose severity level is below the inherited severity level;

subsequent to said logging and tracing controllers writing received messages into their respective log and trace files, correlating the specific locations of software within the enterprise information system to the specific categories of software within the enterprise information system; and,

informing the logging controller that the logging controller is to write received messages into both the log file and the trace file so that the tracing controller is no longer used to write received tracing messages into the trace file.

44. (New) The computer of claim 43 wherein the available security levels further include:

a third severity level whose corresponding messages contain information for debugging;

a fourth severity level that permits its corresponding messages to contain path information for looping and branching;

a fifth severity level whose messages are an echo of what has been performed.

45. (New) The computer of claim 44 wherein the first and second severity levels are higher severity than the third, fourth and fifth severity levels.

46. (New) The computer of claim 45 wherein respective severity levels for at least a portion of the received logging and tracing messages are determined by assigning the respective severity levels to the respective software within the enterprise system that generated the portion of the received logging and tracing messages.

47. (New) The computer of claim 46 wherein the correlating of the specific locations of software within the enterprise information system to specific categories of software within the enterprise information system is submitted through a category application programming interface (API).

48. (New) The computer of claim 47 wherein the informing of the logging controller that the logging controller is to write received messages into both the log file and the trace file is conducted through the messages received by the logging controller that are written into both the log file and the trace file.